대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2002-0066130
Application Number

출 원 년 월 일 : 2002년 10월 29일
Date of Application OCT 29, 2002

출 원 인 : 한국전자통신연구원
Applicant(s) Electronics and Telecommunications Research Inst

2003 년 10 월 02 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0001
【제출일자】	2002.10.29
【발명의 명칭】	강제적 접근 제어가 적용된 보안 운용 체제에서의 신뢰 채널 제공 장치 및 방법
【발명의 영문명칭】	APPARATUS AND METHOD FOR PROVIDING TRUSTED CHANNEL IN SECURE OPERATING SYSTEMS WHICH ARE BY USING MANDATORY ACCESS CONTROL POLICY
【출원인】	
【명칭】	한국전자통신연구원
【출원인코드】	3-1998-007763-8
【대리인】	
【성명】	장성구
【대리인코드】	9-1998-000514-8
【포괄위임등록번호】	2001-038646-2
【대리인】	
【성명】	김원준
【대리인코드】	9-1998-000104-8
【포괄위임등록번호】	2001-038648-7
【발명자】	
【성명의 국문표기】	임재덕
【성명의 영문표기】	LIM,Jae Deok
【주민등록번호】	740101-1450813
【우편번호】	704-915
【주소】	대구광역시 달서구 성당1동 540번지
【국적】	KR
【발명자】	
【성명의 국문표기】	유준석
【성명의 영문표기】	YU,Joon Suk
【주민등록번호】	720624-1079714

【우편번호】 425-825
【주소】 경기도 안산시 사2동 1473-5 301호
【국적】 KR
【발명자】
【성명의 국문표기】 은성경
【성명의 영문표기】 UN,Sung Kyong
【주민등록번호】 680825-1480228
【우편번호】 305-729
【주소】 대전광역시 유성구 전민동 나래아파트 102-703
【국적】 KR
【발명자】
【성명의 국문표기】 두소영
【성명의 영문표기】 DOO,So-Young
【주민등록번호】 700623-2490418
【우편번호】 305-761
【주소】 대전광역시 유성구 전민동 엑스포아파트 304-108
【국적】 KR
【발명자】
【성명의 국문표기】 김정녀
【성명의 영문표기】 KIM,Jeong Nyeo
【주민등록번호】 650919-2565712
【우편번호】 302-727
【주소】 대전광역시 서구 내동 코오롱아파트 8-801
【국적】 KR
【발명자】
【성명의 국문표기】 손승원
【성명의 영문표기】 SOHN,Sung Won
【주민등록번호】 571225-1674514
【우편번호】 305-761
【주소】 대전광역시 유성구 전민동 엑스포아파트 208-902
【국적】 KR
【심사청구】 청구

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인
장성구 (인) 대리인
김원준 (인)

【수수료】

【기본출원료】	20 면	29,000 원
【가산출원료】	8 면	8,000 원
【우선권주장료】	0 건	0 원
【심사청구료】	10 항	429,000 원
【합계】	466,000 원	
【감면사유】	정부출연연구기관	
【감면후 수수료】	233,000 원	

【기술이전】

【기술양도】	희망
【실시권 허여】	희망
【기술지도】	희망

【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명은 강제적 접근 제어가 적용된 보안 운용 체제에서의 신뢰 채널 제공 장치 및 방법에 관한 것으로, 송신 측면에서 송신측 사용자로부터 제공된 통신 요청에 따른 데이터가 패킷 전송 요청일 경우, 신뢰 채널 적용 여부를 판단하여 신뢰 채널이 적용되면, 신뢰 채널 헤더를 구성하고, 패킷의 특정 부분을 암호화하며, 인증 정보를 신뢰 채널 헤더에 저장하여 네트워크를 통해 송신하는 신뢰 채널 서브 시스템; 신뢰 채널 적용 여부에 대한 정보를 제공하는 강제적 접근제어(Mandatory Access Control, MAC) 모듈; 신뢰 채널 서브 시스템에서 신뢰 채널 적용 정보 및 암호, 인증 키 등을 제공하는 커널 메모리; 수신 측면에서 네트워크를 통해 수신된 패킷을 복호화하기 전에 신뢰 채널 헤더 부분의 인증 데이터를 검색하고, 인증 데이터가 유효하면, 암호화된 패킷을 복호화하고, 신뢰 채널 수행에 대한 처리가 끝나면, 상위 레벨의 입력 처리 부분으로 전달하는 루틴을 이용해 패킷을 상위 레벨로 전달하여 수신측 사용자에게 전달하는 신뢰 채널 서브 시스템; 암호화된 패킷의 복호화에 필요한 인증 및 암호 키를 제공하는 커널 메모리를 구비한다. 따라서, 패킷이 전송되다가 악의적인 목적으로 인해 가로채기 당하더라도 암호화가 되어 있으므로 전송되는 데이터의 내용을 알지 못하고, 악의적인 내용으로 대체되더라도 인증 데이터를 통해 무 결성을 검사하므로 변조에 대해 안전하며, 목적지 주소와 사용자의 보안 등급 여부로 신뢰 채널 적용을 결정하고, 적용 대상을 보안 등급을 가진 주체로 제한하여 보안성을 제공함과 동시에 성능 저하를 감소할 수 있는 효과가 있다.

【대표도】

도 1

【명세서】

【발명의 명칭】

강제적 접근 제어가 적용된 보안 운용 체제에서의 신뢰 채널 제공 장치 및 방법{APPARATUS AND METHOD FOR PROVIDING TRUSTED CHANNEL IN SECURE OPERATING SYSTEMS WHICH ARE BY USING MANDATORY ACCESS CONTROL POLICY}

【도면의 간단한 설명】

도 1은 본 발명에 따른 강제적 접근 제어가 적용된 보안 운용 체제에서의 신뢰 채널 제공 장치에 대한 블록 구성도이고,

도 2는 본 발명에 따른 강제적 접근 제어가 적용된 보안 운용 체제에서의 신뢰 채널 제공 방법의 동작에 대한 흐름도이며,

도 3은 본 발명에 따른 신뢰 채널을 적용하면서 발생되는 정보 및 사용자의 보안 정보(class, category)를 저장하는 신뢰채널의 헤더에 대한 구성도이며,

도 4는 본 발명에 따른 신뢰채널 헤더가 적용된 패킷에서 암호화가 적용되는 패킷의 암호화 범위와 인증 검사가 적용되는 인증 범위를 나타낸 도면이며,

도 5는 본 발명에 따른 신뢰 채널이 적용되는 경우에 대하여 도시한 도면이다.

<도면의 주요부분에 대한 부호의 설명>

10, 10-1 : 송/수신측 네트워크 서브 시스템

12, 12-1 : 송/수신측 신뢰 채널 서브 시스템

20 : MAC 모듈 30, 30-1 : 커널 메모리

S1 : 송신측 사용자 S2 : 수신측 사용자

A : 네트워크

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<12> 본 발명은 강제적 접근 제어(Mandatory Access Control : MAC)가 적용된 보안 운용 체제에서의 신뢰 채널 제공 장치 및 방법에 관한 것으로, 특히 강제적 접근 제어의 보안 등급을 이용하여 네트워크에 송신할 패킷을 시스템 내부에서 사용자의 개입 없이 자체적으로 암호화를 제공하고, 또한 수신된 암호화된 패킷을 복호화하여 인증을 수행하는 방식으로 신뢰 채널 기능을 제공하도록 하는 장치 및 방법에 관한 것이다.

<13> 통상적으로, 인터넷 및 네트워크의 발전은 급격하게 상승하고 있는 추세로서, 기업 인트라넷 환경, 즉 그룹웨어, 전자 결재 시스템뿐만 아니라, 개인 네트워크 서비스, 즉 전자상거래, 인터넷 뱅킹 등의 서비스가 증가하고 있다.

<14> 이에 따라, 기업 내의 기밀 자료 전송 및 개인 정보 전송 시, 특히 금융에 관련된 보안 정보(예로, 신용카드 번호, 비밀 번호, 개인 정보 등) 전송의 횟수가 급격하게 증가하는 실정이다. 하지만, 스니핑(sniffing) 및 스푸핑(spoofing) 등의 네트워크 패킷에 대한 해킹 기법 역시 기술적 수준과 해킹 횟수가 꾸준히 증가하고 있음에 따라 이들의 보안 정보에 대한 누출 위험성은 더욱 더 증가하고 있다.

<15> 이러한, 보안 정보에 대한 누출 위험성에 대응하기 위한 기법으로

SHTTP(Secure HyperText Transfer Protocol), SSL(Secure Socket Layer) 등의 솔루션들이 제공되고 있으나, 대부분 특정 서비스에 국한되어 이용되고 있어 네트워크 전반에 걸친 서비스에 적용하기에 무리가 있고, 주로 사용자 수준에서 제공되기 때문에 해킹이나 불안정한 설정 등의 이유로 시스템이 불안정할 경우 데이터의 안전한 전송을 보장하지 못하여 별도의 프로그램의 설치 및 환경 설정 등의 작업이 필요하다.

<16> 또한, 네트워크 통신에 보안성을 제공하는 기법으로는 네트워크 계층 중 인터넷 프로토콜(internet protocol : IP) 계층에서 보안성을 제공하는 IPSec(IP Security) 기술이 대표적으로 이용되고 있다. 이 기법은 가상 사설망(Virtual Private Network : VPN) 등의 네트워크 망에서 보안성을 제공하기 위해 주로 이용되며, IPSec을 구현하기 위한 기법들이 IETF(Internet Engineering Task Force) RFC(Request For Comments) 문서로 표준화되어 사용된다.

<17> 이중, 대표적으로 사용되는 IPSec 보안 프로토콜은 인증 헤더(Authentication Header : AH)와 캡슐화 보안 페이로드(Encapsulating Security Payload : ESP)가 있는데, 이중 데이터의 기밀성 유지를 위해 암호화를 제공하는 것은 바로 ESP이다.

<18> AH와 ESP 모두 IPSec을 이용하기 위해서는 네트워크 트래픽에 보안 서비스를 제공하는 단방향 연결을 의미하는 보안 연계(Security Associations : SA) 개념을 지원해야 한다.

<19> 그리고, IPSec에서 제공되는 패킷 보호는 보안 정책 데이터베이스(Security Policy Database : SPD)에 기반하여 정해지는데, SPD는 사용자나 시스템 관리자가 설정 및 유지하거나, 아니면 이들이 설정한 제약 하에 작동되는 어플리케이션에 의해 설정 유지된다.

<20> 이 패킷들은 SPD의 항에 합치되는 IP나 트랜스포트 계층 헤더 정보에 기반하여 IPSec 보안 서비스를 받거나 폐기되거나 IPSec을 우회하는 세 가지 처리 모드 중 하나를 선택한다.

<21> 상술한 IPSec은 표준화되어 있기 때문에 일반 시스템에 적용되며, 다양한 암호화 및 인증 알고리즘 등의 사용으로 여러 가지 정책을 설정하여 네트워크의 보안을 유지할 수 있다.

<22> 그렇지만, IPSec 구조는 매우 복잡하고 사용하기 위한 환경 설정도 매우 까다롭기 때문에, 관리자의 환경 설정 및 정책 관리가 철저히 이루어지지 않는다면 IPSec에 의한 보안성을 떨어뜨릴 수 있게 되며, 또한 MAC 같은 접근제어가 적용된 운영체제에서 원격에 접속하는 사용자의 접근제어 정보를 전송하는 기능이 없음에 따라 접근제어 정보를 전송하기 위한 새로운 채널 제공 방법의 필요성이 있다.

【발명이 이루고자 하는 기술적 과제】

<23> 따라서, 본 발명은 상술한 필요성에 의해 안출된 것으로서, 그 목적은 MAC의 보안 등급을 이용하여 통신에 사용되는 패킷을 독립적으로 암호화하기 위해 새로운 헤더를 제공하고, MAC의 보안 등급을 이용해 네트워크 성능 저하를 최소화하며, 신뢰 채널이 적용된 커널을 설치하여 적용한 후부터 신뢰 채널 기능을 제공할 수 있도록 하는 강제적 접근 제어가 적용된 보안 운용 체제에서의 신뢰 채널 제공 장치 및 방법을 제공함에 있다.

<24> 상술한 목적을 달성하기 위한 본 발명에서 강제적 접근 제어가 적용된 보안 운용 체제에서의 신뢰 채널 제공 장치는 송신 측면에서 송신측 사용자로부터 제공된 통신 요청에 따른 데이터가 패킷 전송 요청일 경우, 커널 메모리와 MAC 모듈로부터 얻은 정보로부터 신뢰 채널 적용 여부를 판단하여 신뢰 채널이 적용되면, 신뢰 채널 헤더를 구성하고, 패킷의 특정 부분을 암호화하며, 인증 정보를 신뢰 채널 헤더에 저장하여 네트워크를 통해 송신하는 신뢰 채널 서브 시스템; 신뢰 채널 적용 여부에 필요한 사용자 보안 등급 정보를 제공하는 MAC 모듈; 신뢰 채널 적용 여부에 필요한 신뢰 채널 적용 호스트 정보 및 암호, 인증 키를 제공하는 커널 메모리; 수신 측면에서 네트워크를 통해 수신된 패킷을 복호화하기 전에 신뢰 채널 헤더 부분의 인

증 데이터를 검사하고, 인증 데이터가 유효하면, 암호화된 패킷을 복호화하며 신뢰 채널 수행에 대한 처리가 끝나면, 상위 레벨의 입력 처리 부분으로 전달하는 루틴을 이용해 패킷을 상위 레벨로 전달하여 수신측 사용자에게 전달하는 신뢰 채널 서브 시스템; 복호 및 인증에 필요한 암호, 인증 키를 제공하는 커널 메모리를 포함하는 것을 특징으로 한다.

<25> 또한, 상술한 목적을 달성하기 위한 본 발명에서 강제적 접근 제어가 적용된 보안 운용 체제에서의 신뢰 채널 제공 방법은 송신측 사용자에 의해 통신 요청에 따른 데이터가 제공될 경우, 송신측 신뢰 채널 서브 시스템은 제공된 데이터가 패킷 전송 요청에 해당되면, 인터넷 프로토콜(IP) 계층의 패킷 출력 루틴을 수행하고, 신뢰 채널 적용 여부를 알기 위해 송신측 MAC 모듈과 커널 메모리를 검색하여 신뢰 채널 적용 여부를 체크하는 제1 체크 단계; 제1 체크 단계에서 신뢰 채널이 적용될 경우, 송신측 신뢰 채널 서브 시스템은 적용되는 시점에서 발생되는 정보 및 사용자의 보안 정보(class, category)를 저장하는 신뢰채널의 헤더를 구성하는 단계; 신뢰채널 헤더를 구성한 후, 구성된 신뢰채널 헤더에서 암호화된 패킷에 대한 인증 데이터 및 암호화에 필요한 초기 벡터를 제외한 나머지 모두를 암호화한 후, 패킷의 무 결성을 위해 인증 정보를 생성하고 생성된 인증 정보를 신뢰 채널 헤더에 저장하는 단계; 완성된 신뢰 채널 헤더 및 패킷에 대해 IP 계층의 패킷 출력의 나머지 부분인 체크섬(checksum) 및 단편화 처리를 한 후, 네트워크를 통해 하위 레벨의 출력 루틴으로 패킷을 수신측 신뢰 채널 서브 시스템에 제공하는 단계; 네트워크를 통해 수신된 패킷에 대해 수신측 IP 계층의 패킷 입력 루틴에서 패킷에 대해 재조립 처리, 체크 섬 처리를 맞춘 후, 암호화된 패킷을 복호화하기 위해 신뢰 채널 적용 여부를 패킷 헤더의 정보를 통해 검사하여 적용 여부를 판단하는 제1 판단 단계; 제1 판단 단계에서 신뢰 채널이 적용될 경우, 신뢰 채널 서브 시스템에서 패킷을 복호화하기 전에 신뢰 채널 헤더 부분의 인증 데이터를 검색하고, 인증 데이터가 유효하면, 해당 패킷을

복호화하는 단계; 해당 패킷을 복호화한 후, 신뢰 채널 헤더 처리를 수행한 후, 상위 레벨의 입력 처리 부분으로 전달하는 루틴을 이용해 패킷을 상위 레벨로 전달하여 수신측 사용자에게 전달하는 단계를 포함하는 것을 특징으로 한다.

【발명의 구성 및 작용】

<26> 이하, 첨부된 도면을 참조하여 본 발명에 따른 실시 예를 상세하게 설명하기로 한다.

<27> 도 1은 본 발명에 따른 강제적 접근 제어가 적용된 보안 운용 체제에서의 신뢰 채널 제공 장치에 대한 블록 구성도로서, 네트워크 서브 시스템(10, 10-1)과, MAC 모듈(20)과, 커널 메모리(30, 30-1)를 포함한다.

<28> 네트워크 서브 시스템(10, 10-1)은 커널 내의 네트워크 기능을 수행하는 블록으로서, 그 중 네트워크 서브 시스템(10)은 내부적으로 패킷의 암호화를 담당하는 신뢰 채널 서브 시스템(12)을 구비하며, 네트워크 서브 시스템(10-1)은 패킷의 복호화를 담당하는 신뢰 채널 서브 시스템(12-1)을 구비한다.

<29> 송신 측면에서의 신뢰 채널 서브 시스템(12)은 네트워크 통신을 수행하는 송신측 사용자(S1)로부터 통신 요청에 따른 데이터가 제공되면, 제공된 데이터가 패킷 전송 요청에 해당될 경우에는 IP 계층의 패킷 출력 루틴을 수행하고, 패킷 출력 처리가 끝난 후, 패킷 전송을 처리하기 전에 신뢰 채널, 즉 암호화 적용 여부를 알기 위해 커널 메모리(30)와 MAC 모듈(20)을 검색하여 신뢰 채널 적용 여부를 판단한다.

<30> 신뢰 채널 서브 시스템(12)은 신뢰 채널이 적용될 경우, 신뢰 채널에 대한 정보를 유지하기 위해 신뢰 채널 헤더를 구성하는데, 신뢰 채널 헤더를 구성할 경우, 헤더는 새로이 생성되는 것으로, 이 헤더는 암호화된 데이터의 무 결성을 보장하기 위해 인증 데이터 영역, 복호

화를 제대로 하기 위해서 초기 벡터 영역, 올바른 상위 프로토콜 처리를 위해서 다음 프로토콜 헤더 영역, 헤더 길이를 검사하기 위해서 헤더 길이 영역, 암호화에 사용된 패딩 길이를 알기 위해서 패딩 길이 영역, 통신 주체의 MAC 정보를 전달하기 위해서 보안 등급 및 카테고리 영역을 갖으며, 패킷의 특정 부분을 암호화한 후, 패킷의 무 결성을 위해 인증 정보를 생성하고 생성된 인증 정보를 신뢰 채널 헤더에 저장한다. 여기서, 송신측에서는 상기 패킷의 특정 부분을 암호화하기 위한 기준으로 목적지 주소가 신뢰 채널이 적용된 호스트일 경우와, 통신을 요청하는 사용자가 MAC 보안 등급을 가질 경우이다. 이 때, 신뢰 채널 적용 호스트 주소 정보는 커널 메모리(30)로부터, MAC 보안 등급은 MAC 모듈(20)로부터 얻으며, 암호화된 패킷의 헤더에는 신뢰 채널 적용의 의미가 표시된다.

<31> 이후, 신뢰 채널 서브 시스템(12)은 IP 패킷 출력 처리, 즉 패킷에 대한 체크 섬(checksum) 처리 및 단편화 처리를 하고 네트워크(A)를 통해 하위 레벨의 출력 루틴으로 패킷을 송신한다.

<32> MAC 모듈(20)은 전송 처리를 시작하기 전의 신뢰 채널, 즉 암호화 적용 여부에 대한 정보를 강제적으로 접근하도록 제어하며, 커널 메모리(30)는 신뢰 채널 서브 시스템(12)으로부터 제공된 채널 정보를 저장한다.

<33> 한편, 수신 측면에서의 신뢰 채널 서브 시스템(12-1)은 네트워크(A)를 통해 수신된 패킷에 대해 재조립 처리, 체크 섬 처리 및 상위 레벨로 전달하기 전의 모든 처리를 맞춘 후, 패킷 헤더에서 신뢰 채널 적용 표시 부분으로부터 신뢰 채널 적용 여부를 판단한다.

<34> 신뢰 채널 서브 시스템(12-1)은 신뢰 채널 적용, 즉 패킷이 암호화되었을 경우, 패킷을 복호화하기 전에 신뢰 채널 헤더 부분의 인증 데이터를 검색하고, 인증 데이터가 유효하면, 해당 패킷을 복호화하는 반면에, 인증데이터가 유효하지 않을 경우, 해당 패킷을 버린다.

<35> 이후, 신뢰 채널 서브 시스템(12-1)은 해당 패킷을 복호화한 후, 상위 레벨에서의 정상적인 패킷 처리를 위해 신뢰 채널 헤더 처리, 즉 패킷의 길이 조정 및 상위 레벨에서 처리해야 하는 프로토콜 명시 등 신뢰 채널 수행에 대한 처리가 끝나면, IP 입력 처리 부분에서 상위 레벨의 입력 처리 부분으로 전달하는 루틴을 이용해 패킷을 상위 레벨로 전달하여 상위 레벨에서 처리가 이루어질 경우, 해당 패킷을 수신측 사용자(S2)에게 전달한다.

<36> 커널 메모리(30-1)는 수신된 암호화된 패킷의 인증 및 복호화에 필요한 인증, 암호 키를 제공한다.

<37> 도 2의 흐름도를 참조하면서, 상술한 구성을 바탕으로, 본 발명에 따른 강제적 접근 제어가 적용된 보안 운용 체제에서의 신뢰 채널 제공 방법의 동작에 대하여 보다 상세하게 설명한다.

<38> 먼저, 송신측 사용자(S1)에 의해 통신 요청에 따른 데이터가 제공되는지를 판단한다(단계 201).

<39> 상기 판단 단계(201)에서 데이터가 제공되지 않으면, 데이터가 제공되는지를 판단(201)하는 과정을 반복적으로 수행한다.

<40> 반면에, 상기 판단 단계(201)에서 데이터가 제공되면, 신뢰 채널 서브 시스템(12)은 제공된 데이터가 패킷 전송 요청에 해당되는지를 파악하여 해당될 경우, IP 계층의 패킷 출력 루틴을 수행하고, 패킷 출력 처리가 끝난 후, 패킷 전송을 처리하기 전에 신뢰 채널, 즉 암호화 적용 여부를 알기 위해 커널 메모리(30)와 MAC 모듈(20)을 검색하여 신뢰 채널 적용 여부를 체크한다(단계 202).

<41> 즉, 신뢰 채널 적용 여부를 결정하는 내용에 대하여 보다 세부적으로 설명하면, 그 과정은 패킷 입출력 결정을 판단하여 패킷 입력인지, 아니면, 패킷 출력인지를 체크한다(단계 203).

<42> 상기 체크 단계(203)에서 패킷 입력일 경우, IP 헤더 필드 중 다음 프로토콜이 무엇인지를 나타내는 필드가 신뢰 채널 헤더를 나타내는지를 검사한다(단계 204). 상기 검사 단계(204)에서 필드가 신뢰 채널 헤더를 나타내면, 신뢰 채널을 적용한다(단계 205). 반면에, 상기 검사 단계(204)에서 필드가 신뢰 채널 헤더를 나타내지 않으면, 신뢰 채널을 적용하지 않는다(단계 206).

<43> 상기 체크 단계(203)에서 패킷 출력일 경우, 패킷이 전송되는 목적지 주소를 검사하여 목적지 주소가 신뢰 채널 적용 호스트인지를 결정한다(단계 207). 신뢰 채널 적용 호스트 네트워크 주소는 시스템(12)이 초기화 될 때, 신뢰 채널을 적용할 호스트의 네트워크 주소를 설정해 놓은 파일로부터 신뢰채널을 적용할 호스트의 네트워크 주소가 커널 메모리(30)에 적재된다.

<44> 이후, 패킷 송신 시에 신뢰채널 적용을 결정할 단계가 되면 패킷의 목적지 주소와 커널 메모리(30)에 저장되어 있는 주소와 차례대로 비교하면서 패킷의 목적지 주소가 신뢰채널을 적용하도록 설정되어 있는 주소인지를 결정하는데, 패킷의 목적지 주소가 신뢰채널을 사용하는 시스템일 경우, 신뢰채널 적용할 조건이 되어 패킷 송신을 요청한 송신측 사용자(S1)가 보안 등급을 가지고 있는지를 검사한다(단계 208).

<45> 상기 검사 단계(207)에서 목적지 주소가 신뢰 채널 적용 호스트 주소가 아니라면, 신뢰 채널을 적용하지 않는다(단계 210).

<46> 상기 검사 단계(208)에서 보안 등급을 가지고 있으며, 목적지 주소가 신뢰채널을 사용하는 시스템일 경우, 신뢰 채널을 적용한다(단계 209). 여기서, 신뢰채널이 적용될 경우, 처리할 패킷의 헤더 중 다음 프로토콜을 나타내는 필드에 신뢰채널 헤더로 표시해 줌으로써 수신 측에서 신뢰채널이 적용된 패킷인지 아닌지를 알 수가 있는 것이다. 반면에, 상기 검사 단계(208)에서 보안 등급을 가지고 있지 않으면, 신뢰 채널을 적용하지 않는다(단계 210).

<47> 상기 체크 단계(202)에서 신뢰 채널이 적용될 경우, 신뢰 채널 서브 시스템(12)은 도 3에 도시된 바와 같이, 신뢰 채널을 적용하면서 발생되는 정보 및 사용자의 보안 정보(class, category)를 저장하는 신뢰채널의 헤더를 구성한다(단계 211).

<48> 즉, 신뢰 채널 헤더 구성은 신뢰 채널을 제공하는 환경 특성 상 IPSec에서 사용되는 헤더와는 비교적으로 단순한 형태를 갖는데, 강제적 접근제어와 연동되기 때문에 네트워크 통신 주체에 대한 보안 정보의 전달을 가능하게 하기 위한 구조로서, 그 전체 길이는 36bytes(288bit) 크기를 가지며, 신뢰채널 헤더를 구성하는 필드들로는 도 3을 참조하면, 암호화한 데이터에 대한 인증 정보를 가지는 128-bit인증 데이터 필드(Authentication data), 암호화 알고리즘의 암호학적 동기화 데이터로 사용되는 64-bit 초기 벡터 필드(Initial Vector), IP의 상위 프로토콜을 나타내는 8-bit 다음 헤더 필드(Next_hdr), 신뢰채널 헤더의 바이트 단위 길이를 표시하는 4-bit 신뢰채널 헤더의 길이 필드(TCHLEN), 암호화하기 위해 사용된 패딩의 바이트 단위 길이를 표시하는 4-bit 패딩 길이 필드(PLEN), 통신을 요청한 사용자의 MAC 정보를 표시하는 16-bit 보안 등급 필드(MAC class), 64-bit category 필드(MAC category)로 구성되어 있다. 초기 벡터의 길이는 암호화 알고리즘의 암호화 단위에 따라 변경하여 구성할 수 있다.

<49> 그리고, 도 4는 신뢰채널 헤더가 적용된 패킷에서 암호화가 적용되는 패킷의 암호화 범위 및 인증을 수행할 인증 범위를 나타낸 도면으로서, 신뢰채널 헤더는 IP 헤더 바로 다음에 위치하며, 암호화된 패킷에 대한 인증 데이터 및 암호화에 필요한 초기 벡터를 제외한 나머지 뒷부분을 모두 암호화한 후(단계 212), 패킷의 무 결성을 위해 인증 정보를 생성하고 생성된 인증 정보를 신뢰 채널 헤더에 저장한다(단계 213).

<50> 이후, 신뢰 채널 서브 시스템(12)은 IP 패킷 출력 처리, 즉 패킷에 대한 체크 섬(checksum) 처리 및 단편화 처리를 하고 네트워크(A)를 통해 하위 레벨의 출력 루틴으로 패킷을 신뢰 채널 서브 시스템(12-1)에 제공한다(단계 214).

<51> 반면에, 상기 체크 단계(202)에서 신뢰 채널이 적용되지 않을 경우, 단계 214부터 수행한다.

<52> 신뢰 채널 서브 시스템(12-1)은 네트워크(A)를 통해 수신된 패킷에 대해 재조립 처리, 체크 섬 처리 및 상위 레벨로 전달하기 전의 모든 처리를 맞춘 후, 상위 레벨의 입력 처리 부분으로 패킷을 전달하기 전에 패킷 헤더의 신뢰 채널 적용 필드로부터 신뢰 채널 적용 여부를 판단한다(단계 215).

<53> 상기 판단 단계(215)에서 신뢰 채널 적용, 즉 패킷이 암호화되었을 경우, 패킷을 복호화하기 전에 신뢰 채널 헤더 부분의 인증 데이터를 검사한다(단계 216).

<54> 상기 검사 단계(216)에서 인증 데이터가 유효하면, 해당 패킷을 복호화하고(단계 218), 유효하지 않으면 해당 패킷을 버린다(단계 217).

<55> 상기 판단 단계(215)에서 신뢰 채널 미적용 패킷, 즉 패킷이 암호화되지 않을 경우, 해당 패킷을 바로 상위 레벨로 전달하여 정상적인 네트워크 처리가 이루어지도록 한다(단계 219).

<56> 즉, 해당 패킷을 복호화한 후, 신뢰 채널 서브 시스템(12-1)은 상위 레벨에서의 정상적인 패킷 처리를 위해 신뢰 채널 헤더 처리, 즉 패킷의 길이 조정 및 상위 레벨에서 처리해야 하는 프로토콜 명시 등의 처리를 하며, 신뢰 채널 수행에 대한 처리가 끝나면, IP 입력 처리 부분에서 상위 레벨의 입력 처리 부분으로 전달하는 루틴을 이용해 패킷을 상위 레벨로 전달하여 상위 레벨에서 처리가 이루어질 경우, 해당 패킷을 수신측 사용자(S2)에게 전달한다(단계 219).

<57> 참고적으로, 도 5를 참조하면, 신뢰 채널이 적용되는 경우에 대하여 도시한 도면으로서, 어떤 환경에서 신뢰채널이 적용되어 안전한 통신이 이루어지는지를 알 수 있다.

<58> 도 5a는 각각의 범례를 보여주는 도면이며, 도 5b는 신뢰채널이 적용되어 안전한 신뢰채널 통신을 수행하는 경우로서, 신뢰채널이 적용된 시스템 내의 보안 등급을 가진 사용자가 신뢰채널이 적용된 시스템과의 통신을 요청할 경우 사용자가 송신하는 패킷은 자동으로 암호화되어 전송되고, 상대 시스템에서는 수신된 암호화된 패킷이 자동으로 복호화된다.

<59> 도 5c는 신뢰채널이 적용된 시스템들간의 통신이지만, 통신을 하는 사용자가 보안 등급이 없을 경우이며, 도 5d는 신뢰채널이 적용된 시스템 내의 보안 등급을 가진 사용자가 일반 시스템과의 통신을 수행할 경우이며, 도 5e는 신뢰채널이 적용된 시스템 내의 일반 사용자가 일반 시스템과의 통신을 수행할 경우이며, 도 5f는 일반 시스템에서의 사용자가 신뢰채널이 적용된 시스템과의 통신을 수행할 경우로써, 도 5c, 도 5d, 도 5e, 5f에 대해서는 신뢰채널이 적용되지 않는다.

<60> 이러한, 신뢰 채널 적용 정책은 신뢰채널이 적용된 시스템과 그렇지 못한 일반 시스템과의 혼용을 가능하도록 하며, 또한 보안 등급을 가진 사용자에 대해서만 패킷 암호화를 제공함으로 보안 등급을 가진 사용자의 기밀 데이터에 대한 패킷의 보안성을 제공함과 동시에 암호화에 따른 네트워크 성능 저하를 최소화할 수 있는 것이다.

【발명의 효과】

<61> 상기와 같이 설명한 본 발명은 강제적 접근 제어의 보안 등급을 이용하여 통신에 사용되는 패킷을 시스템 내부적으로 암호화하기 위해 새로운 헤더를 제공하고, MAC의 보안 등급을 이용해 네트워크 성능 저하를 최소화하며, 신뢰 채널이 적용된 커널을 설치하여 적용한 후부터 신뢰 채널 기능을 제공함으로써, 패킷 전송 중에 악의적인 목적으로 인해 가로채기 당하더라도 암호화가 되어 있으므로 전송되는 데이터의 내용을 알지 못하고, 악의적인 내용으로 대체되더라도 인증 데이터를 통해 무 결성을 검사하므로 변조에 대해 안전하며, 신뢰 채널을 적용할 경우, 별다른 네트워크 보안 기능의 추가 없이 네트워크를 통해 전달되는 사용자의 패킷을 보호할 수 있으며, 간단한 정책과 패킷 보호에 따른 성능 저하를 최소화할 수 있으며, 강제적 접근 제어가 적용된 보안 커널에 상에서 동작하는 특정한 상황에서 커널과 하나가 되어 동작하므로 간단한 패치 혹은 신뢰채널이 적용된 커널의 설치만으로 동작이 가능하며, 설정 또한 신뢰채널을 적용할 호스트 주소만을 설정해 주면 된다. 또한 정책 자체가 간단하기 때문에 추가되는 헤더의 크기 또한 36-bytes로 크지 않으며, 원격 호스트에서 통신을 요청하는 사용자의 보안 정보를 관리할 수 있으며, 자체적인 헤더를 가지고 커널 내에서 운용되므로, IPSec 기능을 따로 설치하여 연동할 수 있고, 신뢰채널 적용 결정에 대한 정책으로는 목적지 주소와 사용자의 보

안 등급 여부의 확인으로 매우 간단함에 따라 성능 저하를 최소화한다고 할 수 있는 효과가 있다.

【특허청구범위】

【청구항 1】

보안 운용 체제에서의 신뢰 채널 제공 장치에 있어서,

송신 측면에서:

송신측 사용자로부터 제공된 통신 요청에 따른 데이터가 패킷 전송 요청일 경우, 신뢰 채널 적용 여부를 판단하여 신뢰 채널이 적용되면, 신뢰 채널 헤더를 구성하고, 상기 패킷의 특정 부분을 암호화하며, 인증 정보를 상기 신뢰 채널 헤더에 저장하여 네트워크를 통해 송신하는 신뢰 채널 서브 시스템;

상기 신뢰 채널 적용 여부에 대한 사용자 MAC 정보를 제공하는 MAC 모듈;

상기 신뢰 채널 적용 여부에 대한 신뢰 채널 적용 호스트 주소와 패킷 암호화 및 인증 데이터 생성에 필요한 암호, 인증키를 제공하는 커널 메모리;

수신 측면에서:

상기 네트워크를 통해 수신된 패킷을 복호화하기 전에 신뢰 채널 헤더 부분의 인증 데이터를 검색하고, 상기 인증 데이터가 유효하면, 상기 암호화된 패킷을 복호화한 후, 상기 신뢰 채널 수행에 대한 처리가 끝나면, 상위 레벨의 입력 처리 부분으로 전달하는 루틴을 이용해 상기 패킷을 상위 레벨로 전달하여 수신측 사용자에게 전달하는 신뢰 채널 서브 시스템;

상기 신뢰 채널 서브 시스템에 의해 암호화된 패킷에 대해 인증 검사와 복호화에 필요한 인증 및 암호 키를 제공하는 커널 메모리를 포함하는 것을 특징으로 하는 강제적 접근 제어가 적용된 보안 운용 체제에서의 신뢰 채널 제공 장치.

【청구항 2】

제 1 항에 있어서,

상기 패킷의 특정 부분을 암호화하기 위한 신뢰 채널 적용의 기준은 패킷 목적지 주소가 신뢰 채널이 적용된 호스트일 경우와, 통신을 요청하는 사용자가 보안 등급을 가질 경우로 구분하는 것을 특징으로 하는 강제적 접근 제어가 적용된 보안 운용 체제에서의 신뢰 채널 제공 장치.

【청구항 3】

제 1 항에 있어서,

상기 신뢰 채널 헤더를 구성할 경우, 상기 헤더는 새롭게 생성되는 것으로, 상기 새롭게 생성되는 헤더는 암호화된 데이터의 무 결성을 보장하기 위해 인증 데이터 영역, 복호화를 제대로 하기 위해서 초기 벡터 영역, 올바른 상위 프로토콜 처리를 위해서 다음 프로토콜 헤더 영역, 헤더 길이를 검사하기 위해서 헤더 길이 영역, 암호화에 사용된 패딩 길이를 알기 위해서 패딩 길이 영역, 사용자의 강제적 보안 등급을 전달하기 위해서 보안 등급 및 카테고리 영역을 갖는 것을 특징으로 하는 강제적 접근 제어가 적용된 보안 운용 체제에서의 신뢰 채널 제공 장치.

【청구항 4】

제 3 항에 있어서,

상기 새롭게 생성된 헤더가 추가되더라도 네트워크 서비스를 방해하지 않는 것을 특징으로 하는 강제적 접근 제어가 적용된 보안 운용 체제에서의 신뢰 채널 제공 장치.

【청구항 5】

제 1 항 또는 제 3 항에 있어서,

상기 패킷의 기밀성을 위해 IP 헤더, 인증 데이터, 초기 벡터를 제외한 모든 부분을 암호화 영역으로 하는 것을 특징으로 하는 강제적 접근 제어가 적용된 보안 운용 체제에서의 신뢰 채널 제공 장치.

【청구항 6】

송/수신측 신뢰 채널 서브 시스템 및 MAC 모듈을 구비하는 보안 운용 체제에서의 신뢰 채널 제공 방법에 있어서,

송신측 사용자에 의해 통신 요청에 따른 데이터가 제공될 경우, 상기 송신측 신뢰 채널 서브 시스템은 제공된 데이터가 패킷 전송 요청에 해당되면, 인터넷 프로토콜(IP) 계층의 패킷 출력 루틴을 수행하고, 신뢰 채널 적용 여부를 알기 위해 상기 송신측 MAC 모듈과 커널 메모리를 검색하여 신뢰 채널 적용 여부를 체크하는 제1 체크 단계;

상기 제1 체크 단계에서 신뢰 채널이 적용될 경우, 상기 송신측 신뢰 채널 서브 시스템은 적용되는 시점에서 발생되는 정보 및 사용자의 보안 정보(class, category)를 저장하는 신뢰채널의 헤더를 구성하는 단계;

상기 신뢰채널 헤더를 구성한 후, 상기 구성된 신뢰채널 헤더에서 암호화된 패킷에 대한 인증 데이터 및 암호화에 필요한 초기 벡터를 제외한 나머지 모두를 암호화한 후, 상기 패킷의 무 결성을 위해 인증 정보를 생성하고 상기 생성된 인증 정보를 신뢰 채널 헤더에 저장하는 단계;

상기 송신측 신뢰 채널 서브 시스템의 처리가 끝난 후, 인터넷 프로토콜 패킷에 대한 체크 섬(checksum) 처리 및 단편화 처리를 하고 네트워크를 통해 하위 레벨의 출력 루틴으로 패킷을 수신측 신뢰 채널 서브 시스템에 제공하는 단계;

상기 네트워크를 통해 수신된 패킷에 대해 상기 수신측 인터넷 프로토콜 입력 처리에서 상기 패킷에 대해 재조립 처리, 체크 섬 처리를 맞춘 후, 수신측 신뢰 채널 서브 시스템에서 상기 암호화된 패킷을 복호화하기 위해 신뢰 채널 적용 여부를 패킷 헤더의 신뢰 채널 적용 필드를 통해 판단하는 제1 판단 단계;

상기 제1 판단 단계에서 수신된 패킷이 신뢰 채널이 적용될 경우, 상기 패킷을 복호화하기 전에 신뢰 채널 헤더 부분의 인증 데이터를 검색하고, 상기 인증 데이터가 유효하면, 해당 패킷을 복호화하고, 유효하지 않을 경우 해당 패킷을 버리는 단계;

상기 해당 패킷을 복호화한 후, 상위 레벨의 입력 처리 부분으로 전달하는 루틴을 이용해 상기 패킷을 상위 레벨로 전달하여 수신측 사용자에게 전달하는 단계를 포함하는 것을 특징으로 하는 강제적 접근 제어가 적용된 보안 운용 체제에서의 신뢰 채널 제공 방법.

【청구항 7】

제 6 항에 있어서,

상기 신뢰 채널 적용 여부를 결정하기 위해 상기 패킷의 입출력이 패킷 입력인지, 아니면, 패킷 출력인지를 체크하는 제2 체크 단계;

상기 제2 체크 단계에서 패킷 입력일 경우, IP 헤더 필드 중 다음 프로토콜이 무엇인지를 나타내는 필드가 신뢰 채널 헤더를 나타내는지를 검사하는 제1 검사 단계;

상기 제1 검사 단계에서 필드가 신뢰 채널 헤더를 나타내면, 신뢰 채널을 적용하는 단계;

상기 제2 체크 단계에서 패킷 출력일 경우, 통신 요청의 주체가 보안 등급을 가지고 있고, 목적지 주소가 신뢰채널을 사용하는 시스템일 경우 신뢰 채널을 적용하는 단계를 더 포함하는 것을 특징으로 하는 강제적 접근 제어가 적용된 보안 운용 체제에서의 신뢰 채널 제공 방법.

【청구항 8】

제 7 항에 있어서,

상기 제1 검사 단계에서 필드가 신뢰 채널 헤더를 나타내지 않으면, 신뢰 채널을 적용하지 않는 것을 특징으로 하는 강제적 접근 제어가 적용된 보안 운용 체제에서의 신뢰 채널 제공 방법.

【청구항 9】

제 7 항에 있어서,

상기 신뢰채널이 적용될 경우, 처리할 패킷의 헤더 중 다음 프로토콜을 나타내는 필드에 신뢰채널 헤더로 표시하여 수신 측에서 신뢰채널이 적용된 패킷인지 아닌지를 알 수 있는 것을 특징으로 하는 강제적 접근 제어가 적용된 보안 운용 체제에서의 신뢰 채널 제공 방법.

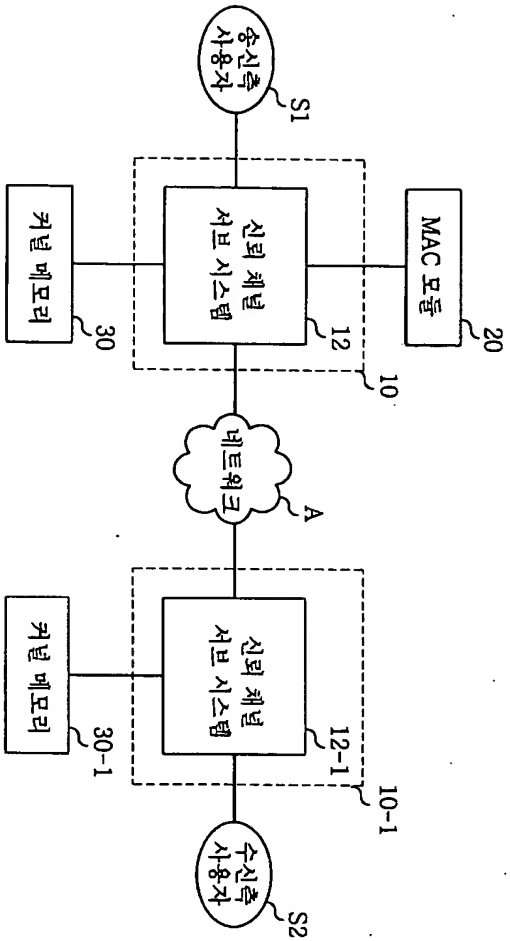
【청구항 10】

제 6 항에 있어서,

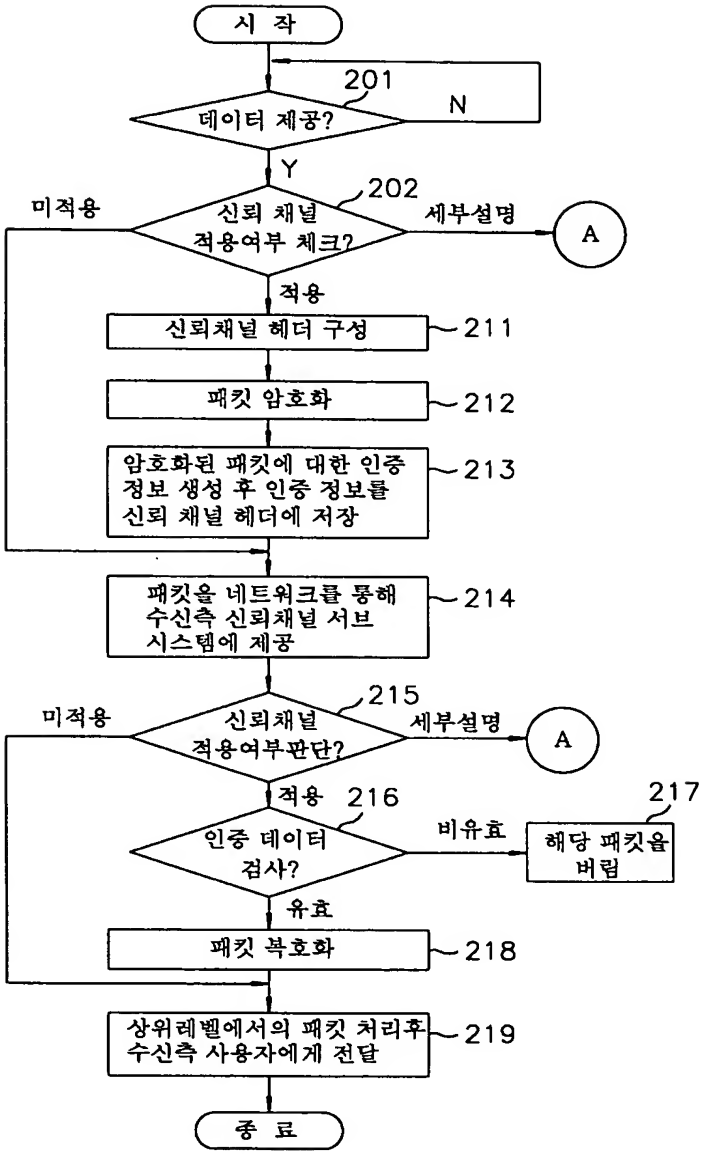
상기 신뢰 채널 헤더 구성은 암호화한 데이터에 대한 인증 정보를 가지는 128-bit 인증 데이터 필드(Authentication data)와, 상기 암호화 알고리즘의 암호학적 동기화 데이터로 사용되는 64-bit 초기 벡터 필드(Initial Vector)와, 인터넷 프로토콜의 상위 프로토콜을 나타내는 8-bit 다음 헤더 필드(Next_hdr)와, 신뢰채널 헤더의 바이트 단위 길이를 표시하는 4-bit 신뢰채널 헤더의 길이 필드(TCHLEN)와, 암호화하기 위해 사용된 패딩의 바이트 단위 길이를 표시하는 4-bit 패딩 길이 필드(PLEN)와, 통신을 요청한 사용자의 강제적 접근제어 정보를 표시하는 16-bit MAC class 필드(MAC class)와, 64-bit category 필드(MAC category)로 구성되어 있는 것을 특징으로 하는 강제적 접근 제어가 적용된 보안 운용 체제에서의 신뢰 채널 제공 방법.

【도면】

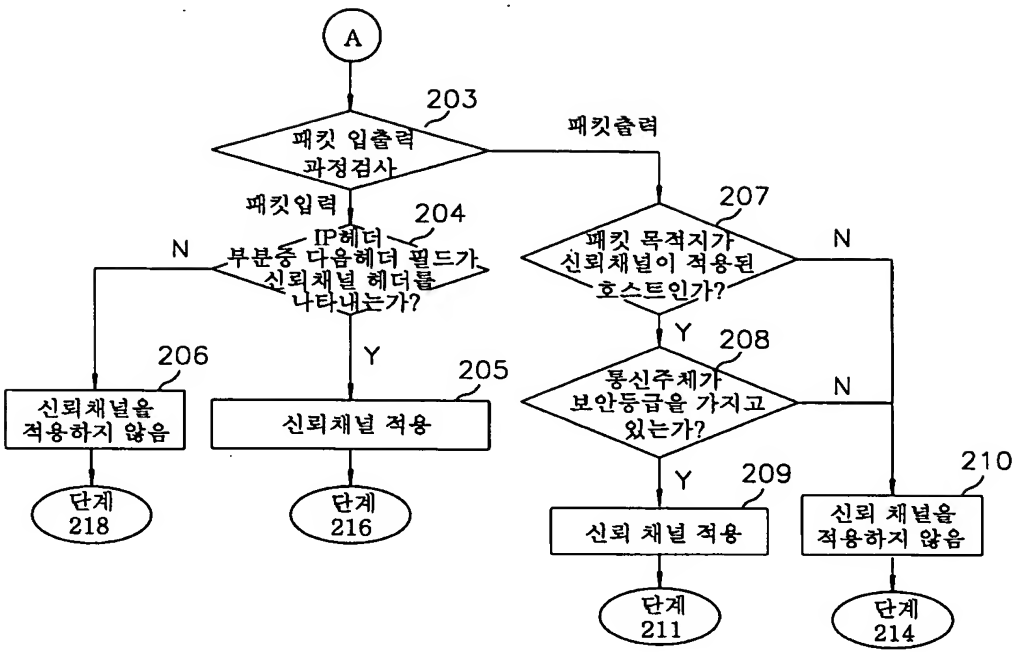
【도 1】


송신측 사용자
S1
신뢰 채널 서브 시스템
커널 메모리
30
MAC 모듈
20
12
10
네트워크
A
신뢰 채널 서브 시스템
커널 메모리
30-1
12-1
10-1
수신측 사용자
S2

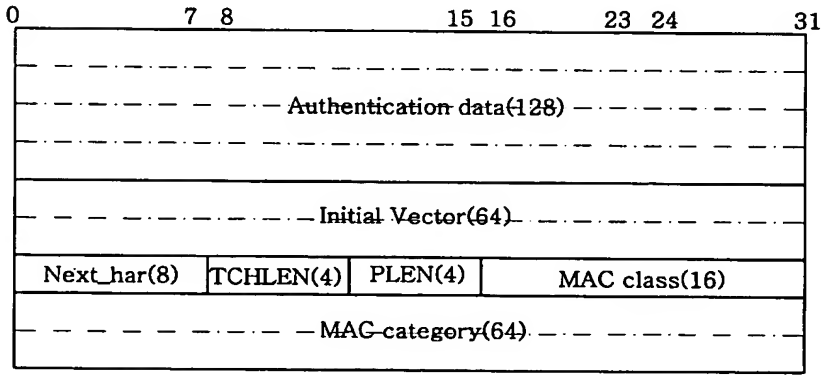
【도 2a】


시 작
201
데이터 제공?
N
Y
202
신뢰 채널 적용여부 체크?
미적용
세부설명
A
적용
신뢰채널 헤더 구성
211
패킷 암호화
212
암호화된 패킷에 대한 인증 정보 생성 후 인증 정보를 신뢰 채널 헤더에 저장
213
패킷을 네트워크를 통해 수신측 신뢰채널 서브 시스템에 제공
214
215
신뢰채널 적용여부판단?
미적용
세부설명
A
적용
216
인증 데이터 검사?
비유효
217
해당 패킷을 버림
유효
패킷 복호화
218
상위레벨에서의 패킷 처리후 수신측 사용자에게 전달
219
종 료

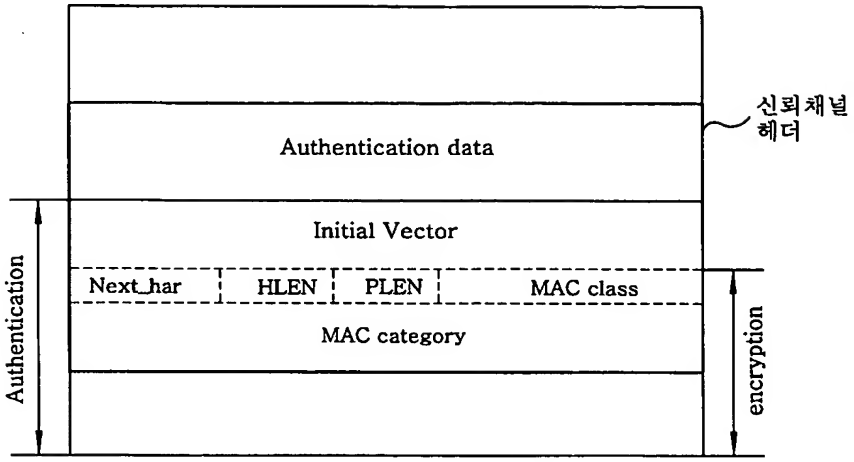
【도 2b】


A
203
패킷 입출력 과정검사
패킷출력
패킷입력
204
IP헤더 부분중 다음헤더 필드가 신뢰채널 헤더를 나타내는가?
N
Y
206
신뢰채널을 적용하지 않음
205
신뢰채널 적용
단계 218
단계 216
207
패킷 목적지가 신뢰채널이 적용된 호스트인가?
N
Y
208
통신주체가 보안등급을 가지고 있는가?
N
Y
209
신뢰 채널 적용
210
신뢰 채널을 적용하지 않음
단계 211
단계 214

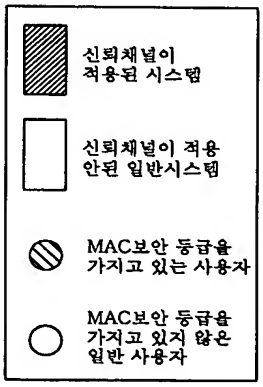
【도 3】


0
7 8
15 16
23 24
31
Authentication data(128)
Initial Vector(64)
Next_har(8)
TCHLEN(4)
PLEN(4)
MAC class(16)
MAC category(64)

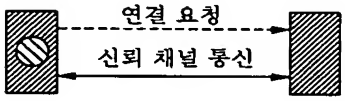
【도 4】



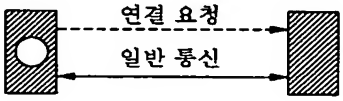
【도 5a】



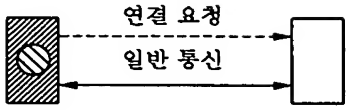
【도 5b】



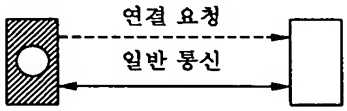
【도 5c】



【도 5d】



【도 5e】



【도 5f】